DESIGNING CRANE CONTROLS WITH APPLIED MECHANICAL AND ELECTRICAL SAFETY FEATURES

Bradford P. Lytle, P. E.; Overhead Bridge Crane Specialist
Chairman, ASME Committee on Cranes for Nuclear Facilities
NASA, Kennedy Space Center

Thomas A. Walczak, P. E.
Critical Control System Consultant
Sugar Land, Texas

Abstract

The use of overhead traveling bridge cranes in many varied applications is common practice. In particular, the use of cranes in the nuclear, military, commercial, aerospace, and other industries can involve safety critical situations. Considerations for Human Injury or Casualty, Loss of Assets, Endangering the Environment, or Economic Reduction must be addressed. Traditionally, in order to achieve additional safety in these applications, mechanical systems have been augmented with a variety of devices. These devices assure that a mechanical component failure shall reduce the risk of a catastrophic loss of the correct and/or safe load carrying capability.

ASME NOG-1-1998, (Rules for Construction of Overhead and Gantry Cranes, Top Running Bridge, and Multiple Girder), provides design standards for cranes in safety critical areas. Over and above the minimum safety requirements of todays design standards, users struggle with obtaining a higher degree of reliability through more precise functional specifications while attempting to provide "smart" safety systems.

Electrical control systems also may be equipped with protective devices similar to the mechanical design features. Demands for improvement of the cranes "control system" is often recognized, but difficult to quantify for this traditionally "mechanically" oriented market. Finite details for each operation must be examined and understood. As an example, load drift (or small motions) at close tolerances can be unacceptable (and considered critical). To meet these high functional demands encoders and other devices are independently added to control systems to provide motion and velocity feedback to the control drive.

This paper will examine the implementation of Programmable Electronic Systems (PES). PES is a term this paper will use to describe any control system utilizing any programmable electronic device such as Programmable Logic Controllers (PLC), or an Adjustable Frequency Drive (AFD) 'smart' programmable motion controller. Therefore the use of the term Programmable Electronic Systems (PES) is an encompassing description for a large spectrum of programmable electronic control devices.

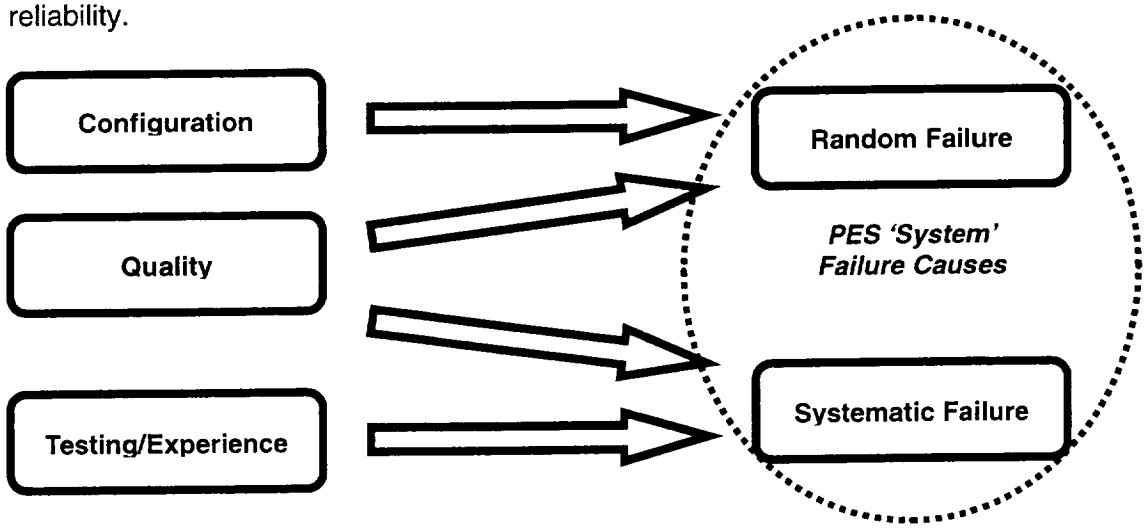
The Programmable Electronic System

Many control systems today are using Programmable Electronic Systems (PES) to process feedback data, detect control errors and respond appropriately (without unacceptable movement of the load). Properly designed control systems provide excellent crane performance and add smart safety features into the control design. Smart control systems can detect many component failures (electrical or mechanical), safely stop the crane/hoist and minimize unwanted motion. If control errors occur, a discontinuity between inputs and control output state can be detected and an appropriate recovery or shut down can occur.

Does this cover ALL the potential failures in the crane system? PES based controls have various internal failure modes as well. Many of these failures might ultimately directly lead to the 'system' failure if not correctly understood. This can occur if the PES system loses its ability to perceive and mitigate a control failure or respond to the failure before an incident occurs. It may be that a failure mode to the system itself is dangerous and cannot be detected and/or responded to so that the resultant action is not maintained fail-safe or fault tolerant. It can be recognized that various scenarios and factors can produce other similar potential inappropriate system actions.

This paper provides a practical look at single-failure-proof crane design as implemented on cranes that support the Space Shuttle program and spacecraft operations at the Kennedy Space Center. This paper also discusses the use of PES in safety critical applications such as overhead bridge cranes and other applications.

Control systems for safety critical applications can include simple independent monitoring systems. However, when a high degree of reliability is required, smart control architectures including dual and triplicate PLC voting systems are available. They are specifically designed for safety critical applications. They can reduce random and systematic PES failures and keep the critical process or operation safe by one, two, or three orders of magnitudes. This high performance equipment utilizing "purpose specific" PES based safety certified systems and control architectures can provide a high degree of availability and reliability.



Addressing System Reliability and Availability Requirements

The Application

The lifting, moving, and assembling of the Space Shuttle, various types of satellites, and parts of the International Space Station occurs on a routine basis at the Kennedy Space Center. Since 1981 there have been over 100 launches of the Space Shuttle. It has carried many hundreds of thousands of pounds of equipment into space. Items like the Hubble Space Telescope and the Galileo Spacecraft are now in orbit around Jupiter.

The construction of the International Space Station includes participation of the United States, 11 European Nations, Japan, Russia, Canada and Brazil. The assembly of the Space Station entails the use of 37 Space Shuttle missions and the launch of 10 unmanned rockets. These will be used to carry some 500 tons of Space Station equipment into space for assembly in orbit. This is of course a formable task that starts on earth.

Safe, error-free processing of the Space Shuttle, satellites and International Space Station components poses many challenges. These operations involve lifting and assembling of high dollar item, one-of-a-kind equipment. Some items like the solid rocket boosters on the Space Shuttle are handled while loaded with live propellants, the largest segment weighing 375,000 pounds (170,000 kg). Other spacecraft are very fragile and assembly for launch requires fine motion control for delicate assembly of parts. Many spacecraft are loaded with liquid propellants and moved several times prior to finding its way into the cargo bay of the Space Shuttle or on top of an unmanned rocket booster. The liquid propellants are highly toxic and explosive. The safety of workers and the protection of the unique equipment are considerations that make the lifting and moving of this hardware critical.

Material handling at the Kennedy Space Center, like the nuclear industry, requires error-free handling of "critical" equipment. The incorporation of enhanced safety features on the overhead cranes make these operations as safe as possible.

It is generally assumed that all parts can or 'will' fail. It is just a matter of 'when', 'where', and 'how' the failure will occur. For "critical" systems the design must accommodate all credible failures of the components to assure that "when" failure occurs the system must fail in a safe state (or in special cases, tolerate the failure and continue to safely operate until the system can shutdown without dangerous effects). This paper will explore the application of these "critical" control systems on overhead bridge cranes and other "critical" systems. *Note: A listing of Nomenclature is found in Appendix A at the end of this document.*

Traditional Crane Design Techniques

Mechanical fail-safe systems have been included in critical crane design for many years. ASME NOG-1-1998, (Rules for Construction of Overhead and Gantry Cranes, Top Running Bridge, and Multiple Girder) provides requirements for mechanical single-failure-proof design features. Design requirements for hoist machinery includes a combination of enhanced safety features. For example, emergency brakes on the wire rope drum, wire rope mis-spooling detection, redundant wire rope reeling systems, dual load paths in the hoisting machinery, dual hoist brakes and increased design factors for components directly in the load path. The mechanical fail-safe features are very important, however electrical fail-safe features are just as important.

One of the primary electrical fail-safe features found in ASME NOG-1-1998 is an emergency stop button for the crane operator. The emergency stop button is electrically isolated from other parts of the control system. Actuation of the emergency stop button removes power to the crane to safely stop all motion. The controls on the crane are fail-safe. Removal of power places each system in a safe state. The power to the hoist motor is removed and the brake coils are de-energized and spring shut, all motion is stopped. No matter what electrical control failure has occurred, the emergency stop system will work correctly. This is an independent system electrically isolated from the rest of the control system. However, this type of arrangement is dependent upon the human element of awareness, recognition, and action.

The Kennedy Space Center requires an additional "layer of protection" to the emergency stop button feature. A "remote" emergency stop button is provided to a person at the point where the load is handled. This "second person" can watch the load in an area different from the crane operator. If something unusual happens the second person can hit the remote emergency stop button and safely stop all motion. Many times when large items are moved, one crane operator cannot see the entire circumference of the load and the many critical interface points, or areas of interference. With the second person the reaction time between spotters and the crane operator can be faster, the second set of eyes that directly "sees" the problem and can react to it with the "remote" emergency stop has been found to be of benefit. The "remote" emergency stop button usually consists of a red mushroom button (with a green ready light) wired to a shunt trip breaker. The breaker shuts off all crane power. Once again however, this type of arrangement is dependent upon the human element of awareness, recognition, and action.

Automated Systems

Enhanced safety systems have been incorporated on mechanical systems for quite some time. However, electrical control systems should not be overlooked. Failure of the control system can cause incorrect load movement, or worse. Today, Programmable Electronic Systems (PES) are being used in critical applications where precise control of the load is needed. Error checking, control diagnostics, and control system emergency shutdown features can be incorporated in the control system. These control systems must be designed correctly in order to provide the enhanced safety features needed.

Safety critical electrical control systems are now addressed by current industry standards such as those found in the IEC 61508 "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety–Related Systems" or the ANSI/ISA S84.01 "Application of Safety Instrumented Systems for the Process Industry". The control industry has available "Safety Critical" control systems with a "purpose specific" design for these types of critical applications.

The Safety Issue

There are several safety systems on the crane that remove power from the crane providing a fail-safe protection. An automated electrical fail-safe control system is not required by ASME NOG-1-1998 or other industry specifications.

However, failures can occur in the PES based control system such that the crane operator (or "remote" emergency stop operator) cannot react in time to prevent critical load movement due to the failure. Understand, all parts are assumed to fail, it's just a mater of when. Damage to "critical" equipment or the safety of personnel can be placed at risk. In this case the control system must be designed to tolerate all credible failures. An automated control system designed to detect a control failure and provide safe system shutdown would be required.

The application of a PES in "critical" control systems provides many capabilities that are needed, such as; fine positioning, velocity control and safety monitoring. However, if the system is not designed properly the PES system can directly lead to failure of the critical system.

Applied Solid-State and Microprocessor Considerations

Because of certain inherent PES failure-modes, control systems designed using a single PES control architecture are at risk for erroneous operation which could cause the control system, or an end device, to operate in a dangerous manner.

Failure modes inherent to microprocessors and their associated peripherals have the potential to allow the issuance of multiple unsolicited output signals, or can fail to sense critical inputs. This can result in erroneous computations or other forms of erratic operation. Although most PLC's have some form of internal diagnostics, watchdog timers and the like, few, if any, are totally immune to failures that can disable the internal logic solver components. Simply speaking, the PLC can fail to become aware it has failed and may not be able to prevent an unwanted event (fail-to-danger). Even if we "program" the PLC to perform safing functions in the event of failure, the problem that caused the PLC to malfunction in the first place could end up being the same problem that will not allow the PLC to perform the safing routine. *In generic terms, it must be understood that ANY programmable electronic device can fail in any of the above mentioned ways. This condition is true for personal computers, PES/PLC's or any other type of microprocessor based device.*

For this reason, we must ensure that usage of PES in control system architectures employs a suitable method of fail-safe protection. A Safety Instrumented System (SIS) is a term becoming familiar in the process control industry, which describes an acceptable method of fail-safe protection that is totally independent of the Basic Process Control System (BPCS). A SIS contains an independent electronic or electromechanical method that will detect and mitigate a critical failure in the BPCS.

Note: It should remain clear that a SIS mechanism is NOT meant to be a "redundant" (or secondary) system to the basic control system! The sole purpose of a SIS is to prevent an unwanted/unsafe condition if the basic control system fails. Ideally, the SIS should be designed only to recognize control system failure, prevent unsafe conditions and command the system to a safe state. However, a redundant system can in certain circumstances, and if implemented correctly, be used as a method for employing a SIS.

Fail Safe and Fault Tolerance

A typical "fail-safe" Emergency Safety System (ESS) is designed in such a way that zero or de-energized is the safe state. As soon as a fault is detected, the system is de-energized/shuts down to its safe state. Almost all systems on cranes provide this type of fail-safe designed system.

A Continuous Control System must detect a failure and an alarm must be generated (while an instantaneous shutting down of the system may not provide the increased safety). Instead, the control process might continue and additional steps must be taken to bring the system to a final safe state. The system is required to tolerate the fault and continue to operate safely. In either case, the control systems must appropriately respond to the failure and provide a means to command the system to a safe state.

Control System Configuration

An illustrative example can be used to describe a correct and an incorrect application of the SIS. The incorrect application is illustrated in Fig. 1.

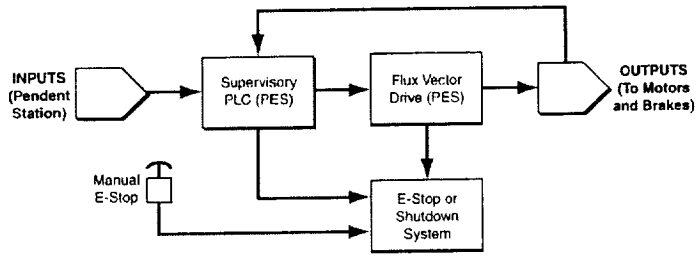


FIGURE 1. SERIAL PES CONFIGURATION
(INCORRECT APPLICATION)

Here a crane control system uses a PLC and a Flux Vector Drive as the crane's Basic Process Control System. The PLC receives input from the pendent control switches. The PLC reads the command inputs from the pendent station and issues it's control output response to the Flux Vector Drive. The Flux Vector Drive then provides drive current to the motors and brakes.

Feedback from encoders mounted on the motors is provided to the PLC to allow the PLC to recognize an errant condition in an output or in the Flux Vector Drive system and shutdown the crane operating power. However, a malfunctioning PLC could originate an errant command. We are then left without a method to provide safe shutdown of the system. In addition, the PLC has no way to detect a failure in its input modules. A failure could occur in the input module that would cause the PLC to recognize and respond to a command that hasn't really been given by the operator. Both the PLC and the Flux Vector Drive can be considered "smart" devices, but they are arranged in a *serial* configuration. This configuration could allow a failure to propagate "downstream" without detection or mitigation.

The original PLC / Flux Vector Drive design concept was intended to be "fail-safe." The PLC was intended to guard against pendent switch or Flux Vector Drive failure. This concept employs two smart devices in series (Serial PES Configuration). Each item is generally considered 80% "fail-safe," (20% probability that if the item fails it could result in a fail-to-danger scenario). Therefore, the resultant reliability of the two items in series is lower than 80% fail-safe.

Serial PES Configuration is the basic example of incorrect control design (Fig. 1). Will the Primary Control PLC sense incorrect inputs? How smart is the Flux Vector Drive? We cannot answer those questions. Instead of improving system integrity the addition of the supervisory PLC has added another means of failure, it degrades the system integrity and does not enhance it.

Below in figure 2, the hardware was reconfigured and placed in parallel where the supervisory PLC can be used for strictly monitoring the Flux Vector Drive (the Basic Process Control System) in lieu of monitoring and commanding the system at the same time. The inherent reliability and safety integrity is greatly increased. This type of architecture constitutes a Safety Instrumented System (Fig. 2).

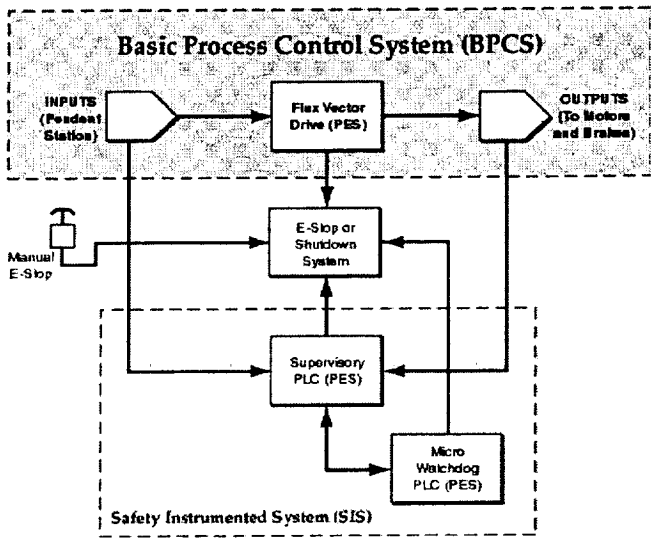


FIGURE 2. SAFETY INSTRUMENTED SYSTEM (SIS)

The desired solution is a design with inherent safety and reliability so that microprocessor failure cannot result in a fail-to-danger occurrence. A Safety Instrumented System, also called a Safety Interlock System, can be defined as an instrumented and automated layer of protection usually contained in a Programmable Electronic System (PES) and separated from the Basic Process Control System (BPCS). It is dedicated to prevent unwanted control responses. The SIS can be described as an independent supervisory circuit that monitors critical aspects of the BPCS and independently controls the emergency shutdown system.
In order to meet fail-safe or single-failure-proof requirements for PES based control systems, a SIS must be used.

A SIS may include a PES based system that monitors critical inputs and outputs of the BPCS. If an input or output falls outside a set of accepted limits, the PES can shut the control system down, or place the system in a safe mode of operation. Figure 2 also depicts the illustrative example where feedback is provided to the independent processor PLC through an encoder. The independent processor (PLC) compares input commands to the outputs (actual crane motion). The independent processor PLC can initiate a system shutdown if an out of tolerance motion is detected. Furthermore, a Micro Watchdog PLC (a microprocessor watchdog circuit) watches the "heartbeat" of the independent processor PLC to assure it is functioning correctly. The cost and programming of this watchdog PLC is very small but it assures correct system function and can initiate an independent shutdown if needed. This completes the correct application of the Safety Instrumented System.

Question: Is a Programmable Electronic System (PES) as an SIS always the required layer of protection necessary to reduce risk to a sufficient level? No. A "hard wired safing system" (a manual "off switch" such as the emergency stop button on a crane) can satisfy fail-safe needs. However, in all cases the "hardwired safing system" must shut down the system to a known safe state. It must be independent of the Basic Process Control System (BPCS). Any failure within BPCS must not inhibit the ability of the "hardwired safing system" to function. Also, the operator must be cognizant of all failure modes in order to actuate the hardware safing system and have time to react to the failure.

Increasing System Reliability

Critical systems can have varying degrees of criticality. In order to provide maximum protection against critical failures, simply providing Safety Instrumented System control architecture may not be enough. The SIS can be designed as a stand-alone high-reliability system in order to ensure to the greatest degree, that it WILL perform its SAFING functions when required, or tolerate a failure and continue to function correctly until proper safe shutdown can be achieved. It must be understood that every type of electrical device will eventually fail, including the components in the SIS. It's just a matter of when. For this reason the process control industry has been developing a new generation of high-reliability PES's that are specifically intended for SIS applications. These devices contain a high degree of internal hardware and firmware diagnostics that provide continuous real-time diagnostic testing and shutdown capability. Some of these PES's have been laboratory certified, by TÜV Rheinland, for stand-alone use in critical applications. However, not even a high-reliability PES is totally immune from failure!

Standards, Testing, and Certification

A TÜV Certified Programmable Logic Controllers (PLC) is one that has been tested and approved for use in critical systems by TÜV Rheinland, an independent testing and certification agency (similar to Underwriters Laboratory). They are tested against standards such as those found in the IEC 61508 and the ANSI/ISA S.84. Additionally, other standards like the EN, NFPA, DIN, and VDE standards may be the basis for testing. Such certifications are given only to PLC's that have been field and laboratory tested to extreme performance standards.

To obtain such a rating, devices are specially designed with additional internal circuitry and firmware, which guard against most internal failures (>99%) that could cause the device to fail-to-danger. Although 99% fail-safe, a single device is not single-failure-proof. THIS IS TRUE EVEN THOUGH THE RELIABILITY OF A SIMPLY DESIGNED "FAIL-SAFE" OR "SINGLE-FAULT-TOLERANT" SYSTEM COULD HAVE AN OVERALL LOWER RELIABILITY THAN THE SINGLE TÜV RATED MICROPROCESSOR BASED SYSTEM! Use of a TÜV certified PLC in a SIS however, will increase the overall fail-safe reliability to very high levels.

TÜV Rheinland has been in this business for about 30 years, and has been studying electronic failures and their countermeasures. This is a German based company that has amassed a great depth of knowledge and experience. Currently, there are several TÜV Safety Certified PLC's on the market. With these systems the probability of failing to danger is very low; they contain tested and proven hardware, firmware, and diagnostics. The additional costs of the TÜV Safety Certified PLC over the cost of the non-safety certified "general purpose PLC" is of concern to some, but understand that the system architecture is already designed (the designer does not need to develop system architecture, design system software, or test the two). Initial design cost and continuing development costs will be less. This should justify the cost of the TÜV certified equipment. More about TÜV Rheinland can be found on their web site www.tuvglobal.com (including a list of companies that market TÜV Safety Certified PLC's).

A general purpose PLC is not specifically designed for safety applications. Manufacturers provide warnings and restrictions of how, if at all, the PLC's are used in a critical application. Many PLC's are on the market, and each has its own specific restrictions. TÜV certified PLC manufacturers publish the TÜV restrictions within their user documentation. This ensures that everyone knows about the restrictions for the use of a PLC so it can be applied correctly in the critical applications. These restrictions must be followed to ensure the whole system complies with the manufacturers requirements for critical applications.

System Architecture

Several control architectures are available from industry for critical applications. In order to mitigate single-failure-points inherent with microprocessor based systems, a voting system may be used where two or more PES "vote" on input data and output data so the correct information is processed and utilized. Fault detection routines are used to detect failures to either provide safe shutdown, or in more sophisticated systems ignore false data and continue safe operating (until safe shutdown is possible). Several PES control manufacturers have developed these systems. They vary in their complexity capability and application.

The short hand designation for this system architecture includes a number followed by the lower case letters "oo" and another number. The "oo" means "out of," so, for example, a "1oo2" means a control architecture that selects one vote "out of" two input votes (in short "1 out of 2") necessary for a "trip" or shutdown signal to be valid. A "D" is sometimes added to the end of the notation to represent "with diagnostics." A 1oo2D system provides internal and external diagnostics to the voting PLC's so internal component and field device failures can be detected before they are commanded to operate.

A third type of control architecture called Triple Modular Redundant (TMR) is also available. This will be described below. In all, there are five major types of critical control architecture for most industrial applications. These are 1oo1D, 1oo2, 1oo2D, 2oo2, and TMR.

The following is a brief description of three general systems:

Figure 3 shows the general arrangement of the Duplex 1oo2 voting system. Reading from left to right, dual inputs are read from field devices, data from both is sent to two separate logic solvers. Each logic solver compares results and provides separate output votes to

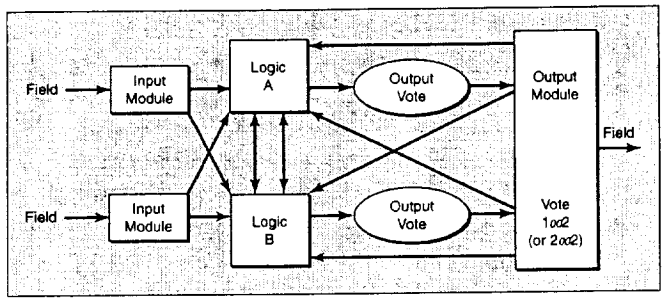


FIGURE 3. DUPLEX 1oo2 VOTING

the output module. The output module does not issue the output until a comparison is made to the logic solver that the correct output votes are in agreement. Here one out of two commands are required to shutdown the system. This provides a decrease in the probably of a fail-to-danger scenario.

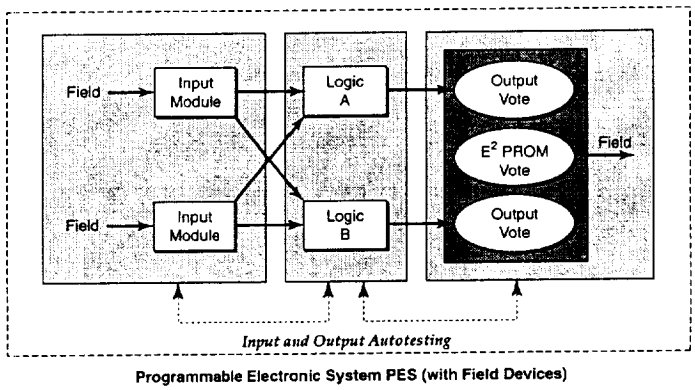


FIGURE 4. DUPLEX DEFAULT VOTING 1oo2D

Diagnostics can be added to improve the system integrity as shown in the 1oo2D system of Fig. 4. Diagnostics in the controllers are used to check the health of internal systems, and for failure of an input module or a field device. The final output is through one out of two serial switches of the controller. This forces the output to a fail-safe state upon failure of any controller. With this system, a high degree of diagnostic coverage is required. To fail, simultaneous failure of two CPU's must occur.

Figure 5 shows the concept of Triple Modular Redundant (TMR) architecture. This provides three sets of input hardware (data collection) and 2oo3 majority voting is used to determine an output. A single component failure can be detected but does not cause a system shutdown. With this system, a failure can occur and the system can continue to operate. The three examples briefly described here show some of the safety critical control architectures that are available from industry. TÜV Rheinland for example, has certified many of these systems for several manufacturers.

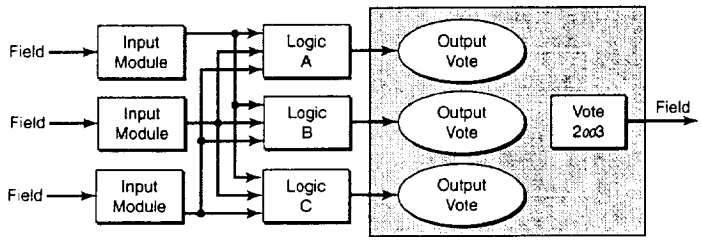


FIGURE 5. 2oo3 TMR VOTING

These systems are designed, certified and ready to be used in the safety critical application that is best suited for its particular features.

Conclusion

The failure of a programmable electronic system (PES) could result in simultaneous multiple output failures. The microprocessor-based system cannot rely upon itself to detect its own failure and then take action to protect itself unless specifically embedded functionality is applied within the design. When the failure of an electrical, electronic, or programmable electronic system results in a critical effect, the design must include a Safety Instrumented System (SIS) capable of providing fail-safe or single-fault-tolerant protection that is independent of the Basic Process Control System (BPCS). An independent microprocessor must be used to detect the failure and take independent action to provide system protection. Critical system design must take into account the understanding "all parts will fail... it is just a matter of when they will fail."

A manual hardwired safing system can provide protection against systems failures but the operator must be cognizant of the failure and have time to react to it. Automated fail-safe systems must otherwise be used.

The control industry has developed several PES based voting systems that use two or more independent logic solvers to assure inputs are read correctly, data is processed correctly, and command outputs are correct. This will provide enhanced safety for critical systems when a failure occurs.

The International Electrotechnical Commission (IEC) has approved all seven parts of the IEC 61508, and the International Society for Measurement and Control (ISA) has developed and approved the ISA S84.01 for such critical applications. These standards should be used so proper design is established for the critical systems.

TÜV Rheinland certifies safety critical control systems for several control manufacturers. This provides cost effective, high reliability systems for many areas where enhanced safety is needed. As a result, PES based systems provide inexpensive control with superb capabilities and their use has become widespread. However, when these systems are used in safety critical applications they must be applied properly as directed by the manufacturer and the certification agency. Failure modes of these systems must be part of the system application design. The systems and industry pre-certifications needed to protect against microprocessor based systems failure are available today and should be used for the safety critical application.

Contact the authors:

Bradford P. Lytle, P. E.; Overhead Bridge Crane Specialist
Chairman, ASME Committee on Cranes for Nuclear Facilities
NASA, Kennedy Space Center; Mail Code: YA-D1
Kennedy Space Center, Florida 32899 U.S.A.
Phone: (321) 867-8539
FAX: (321) 867-2758
E-mail: bradford.lytle-1@ksc.nasa.gov

Thomas A. Walczak, P.E.
Critical Control Systems Consultant
3506 Highway 6 South; Suite 361
Sugar Land, Texas 77478-4401 U.S.A.
Phone: (713) 851-9170
FAX: (281) 980-5391
E-mail: globalemail@alltel.net

REFERENCES

ASME NOG-1-1998, "Rules for Construction of Overhead and Gantry Cranes, Top Running Bridge, and Multiple Girder," American Society of Mechanical Engineers, ISBN: 0-7918-2584-1
ISA S84.01.1996 "Application of Safety Instrumented Systems for the Process Industries," Instrument Society of America Standards and Practices, ISBN: 1-55617-590-6
IEC 61508, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety–Related Systems, 1999, International Electrotechnical Commission
SIS-2000 (Training Course) Integrated Process Risk Management, Thomas A. Walczak Instructor, March 1999
Storey, N., "Safety-Critical Computer Systems," Addison-Wesley Longman, Inc., 1996, ISBN: 0-201-42787-7

APPENDIX A

1oo2 voting - Voting 1oo2 (1 "out of" 2), either vote in an "off" state shall cause the final element to be de-energized "off."
1oo2D voting - The "D" is used to denote diagnostic shutdown detection on the failure of an offending component and will enhance overall reliability.
2oo3 voting - Voting 2oo3 (2 "out of" 3), when 2 of the 3 votes are in an "off" state, the final element will be de-energized "off."
ASME - American Society of Mechanical Engineers.
Basic Process Control System (BPCS) - the primary automated process control system.
Diagnostics - The ability of a control system to provide active mechanisms which can detect both latent and apparent faults.
Duplex - Two Parallel elements in a voting system.
Emergency Stop (E-Stop) - an independent emergency shutdown button (power off button) located at the crane operators pendent or control station. The emergency stop circuit shall be separate and take precedence over the operator control circuits.
Fail-to-danger - The inability of a system to be able to respond safety due to a failure within the control hardware.
Fail-safe - The operational ability of the final element to go to a safe state when a system failure has occurred.
Fault-tolerant - systems have internally redundant parallel components and integral logic for identifying and bypassing faults without affecting the output. If a single element fails, the system will continue to remain functional as if no fault had occurred. The diagnostics will report the fault to the proper location. "Fault-tolerant" and "Redundant" are sometimes used interchangeably. A distinction should be made between the two. "Redundant" and "fault tolerant" systems can be used to make a system "fail-safe," or a control system that is used to bring a controlled process to a pre-defined "safe" state.
IEC - International Electrotechnical Commission.
ISA - International Society for Measurement and Control.
KSC - Kennedy Space Center, Florida, U.S.A.
NASA - National Aeronautics and Space Administration

Programmable Electronic System (PES) - any control system utilizing any programmable electronic device (a microprocessor based device) such as a Programmable Logic Controller (PLC), or an Adjustable Frequency Drive (AFD). This term is intended to encompass a large spectrum of programmable electronic control devices.
Programmable Logic Controllers (PLC) – a solid-state industrial control device that receives singles from user supplied control devices, such as switches and sensors. Then implements them in a precise pattern determined by ladder logic based application programs stored in user memory, and provides output for control of processes or user-supplied devices such as relays or motor starters. It is usually programmed in relay ladder logic and is designed to operate in an industrial environment.
Redundant - systems with individually specified duplicate components and manual or automated means for detecting failures and switching to back-up devices. See "Fault-Tolerant" for additional discussion on this term.
Reliability - The probability that the system, does not fail, and will perform as originally installed at time, *t=0*, during the required operational period.
"Remote" Emergency Stop - An independent emergency stop button on a crane that is used at the level where the load is handled to provide additional visibility to critical areas, and provides emergency stop capability.
Safety Instrumented System (SIS) – Any portion of the control system which contains safety critical instrumentation.
Safety Integrity Level (SIL) - a safety rating that provides a quantitative characteristic of system failure rates. This is defined in ISA S.84.01 and IEC 61508.
Triple Modular Redundancy (TMR) - Using 2oo3-voting techniques provides an architecture that can be configured as fault-tolerant and fail-safe. Only systems, which are fault-tolerant and fail-safe, may be considered a true safety TMR system.
TÜV Rheinland - TÜV is an acronym for a German name Technisher Überwachungs-Verin (in English this loosely translates to Technical Supervisory Association). This is a technical inspection and testing agency that operates many offices worldwide (web site www.tuvglobal.com).
Underwriters Laboratory (UL) - A testing laboratory with international capability to certify electronic hardware.
Voting - The ability for a system to automatically majority vote independent signals received, and place the voted solution in a separate region of memory.
Watchdog timer - A timer in the CPU used to ensure certain hardware conditions are met within a predetermined time. End.

This paper is adapted from the Proceedings of ICONE 8, the 8th International Conference on Nuclear Engineering, April 2-6, 2000, Baltimore, MD USA. ICONE-8547 Cranes at NASA'S KENNEDY SPACE Center Utilizing Enhanced Mechanical and ELECTRICAL SAFETY Features